

**Listing of Claims:**

1. (Currently Amended) A method for encrypting and decrypting copyrighted electronic contents data to be distributed from a server to a user terminal through a network, said method comprising:

5       receiving from the user terminal contents specifying data specifying the copyrighted electronic contents data to be distributed;

retrieving, from a contents database, contents information comprising at least one of a size of the copyrighted electronic contents data and a preceding update date of the copyrighted  
10 electronic contents data based on the received contents specifying data;

      generating a first key at the server from the retrieved  
contents information relating to the copyrighted electronic  
15 contents data to be distributed;

      generating a second key at the server from: a variable parameter received from the user terminal, a H/W key ID retrieved from a user information database by using a user ID received from the user terminal, and said first key, and then sending the  
20 generated second key to the user terminal;

      decrypting the first key at the user terminal from the variable parameter, the H/W key ID, and said second key;

encrypting the contents data to be distributed at the server  
by using said first key and sending the encrypted contents data  
25 to the user terminal; and

decrypting the encrypted contents data at the user terminal  
by using said decrypted first key.

2. (Previously Presented) The method according to claim 1,  
further comprising generating the variable parameter at the user  
terminal and sending the generated variable parameter to the  
server.

Claim 3 (Canceled).

4. (Previously Presented) The method according to claim 1,  
further comprising synchronizing the variable parameter between  
the user terminal and the server.

5. (Original) The method according to claim 4, wherein said  
synchronization between the user terminal and the server is  
performed at a time different from a time when the contents data  
is distributed.

6. (Currently Amended) A contents data encrypting and  
decrypting system comprising:

(i) a server which comprises:

means for receiving contents specifying data specifying  
5 copyrighted electronic contents data to be distributed,

means for retrieving, from a contents database,  
contents information comprising at least one of a size of the  
copyrighted electronic contents data and a preceding update date  
of the copyrighted electronic contents data based on the received  
10 contents specifying data;

means for generating a first key from the retrieved  
contents information relating to the copyrighted electronic  
contents data to be distributed,

means for generating a second key from a variable  
15 parameter, a H/W key ID, and said first key, and

means for encrypting the contents data to be  
distributed by using the first key; and

(ii) a user terminal which comprises:

a network interface configured to send said contents  
20 specifying data to said server, and to receive said second key  
and said encrypted contents data from said server,

means for decrypting the first key from the variable  
parameter, the H/W key ID, and said second key, and

means for decrypting said encrypted contents data by  
25 using said decrypted first key;

wherein the server receives the variable parameter from the  
user terminal, and the server retrieves the H/W key ID from a

user information database by using a user ID received from the user terminal, in order to generate the second key.

7. (Previously Presented) The contents data encrypting and decrypting system according to claim 6, further comprising means for synchronizing the variable parameter between said server and said user terminal.

8. (Currently Amended) A user terminal used in a system in which copyrighted electronic contents data to be distributed from a server to the user terminal through a network is encrypted and decrypted, said user terminal comprising:

5       a network interface configured to send contents specifying data, which specifies the copyrighted electronic contents data to be distributed, from the user terminal to the server, which retrieves, from a contents database, contents information comprising at least one of a size of the copyrighted electronic contents data and a preceding update date of the copyrighted  
10       electronic contents data based on the received contents specifying data, and to receive from the server (i) a second key generated at the server from: a first key generated from the retrieved contents information relating to the copyrighted  
15       electronic contents data to be distributed, a variable parameter received by the server from the user terminal, and a H/W key ID retrieved by the server from a user information database by using

a user ID received from the user terminal, and (ii) the contents data encrypted by using said first key; and

20       a decrypting section configured to decrypt the first key from the variable parameter, the H/W key ID, and said second key, and then to decrypt said encrypted contents data by using said decrypted first key.

9. (Previously Presented) The user terminal according to claim 5, further comprising means for synchronizing the variable parameter between the server and the user terminal.

Claims 10-12 (Canceled).